**UNITED STATES PATENT APPLICATION**

*of*

**Fred Messinger**

and

**George Swallow**

*for*

# NETWORK TRAFFIC VISUALIZATION

# NETWORK TRAFFIC VISUALIZATION

## FIELD OF THE INVENTION

This invention relates to network management applications that assemble network information, and specifically to a visualization application that displays network traffic information assembled by the network management applications.

## BACKGROUND OF THE INVENTION

Distributed computer networks, to which this invention applies, are systems comprising a number of components such as printers, computers, routers and the like, that are interconnected to enable communication among the components and sharing of data and resources. For example, a distributed computer network may include a combination of separate local area networks (LAN) that are connected in a wide area network (WAN) to form a single distributed network structure. The LANs are interconnected to communicate with each other by routers. Each LAN may include servers and clients that are connected by physical media such as cables and network cards in order to share resources such as files or applications. A server may be a computer or process that provides shared network resources to network users and a client is usually a computer that accesses the shared network resources provided by the servers. Shared resources in a network may include printers, other peripherals and software applications.

Network activity information relating to messages transmitted over the network is commonly stored in designated network information files on one or more of the network's computers. As activity information is received from the various network components, it is appended to these files. Records in the files are time stamped to indicate when they were received. The information files thus maintain a record of all activities over the network over some period of time.

In order to view the network activity for a particular computer or group of computers, facilities are commonly provided to retrieve selected data for examination by the user. Such data may include, for example, the amount of traffic into or out of a particular resource in the system; a record of particular kinds of traffic; the identity of traffic originators, etc. Typically, the data is presented in tabular form, and the amount of data can be overwhelming. Thus, it is often difficult to assimilate the data presented. In order to facilitate assimilation of the data, the amount of data may be selectively reduced in volume, but this correspondingly diminishes the information that can be gleaned from it. Most often, such a reduction involves selecting a subset of the data based on the source and/or destination of the data. While such views are interesting in and of themselves, they fail to present a comprehensive, gestalt view of the network

## SUMMARY OF THE INVENTION

We have created a visualization application which enables a user such as a system administrator to rapidly obtain and assimilate substantial amounts of information about various types of transactions involving the respective activities of the components. In particular, in accordance with the present invention, information concerning various aspects of network traffic is monitored and stored for subsequent retrieval and use. For example, the information may be collected by one or more routers through which the data passes as it transits the network, and stored in a separate file from which it is subsequently retrieved for display.

The user may select for display specific subsets of the collected information, as well as specific attributes of these subsets. The criteria for specifying the data may include, among other elements, the identification of particular components whose activity is to be monitored; the starting and ending times of the interval over which the information is to be monitored for subsequent display; the frequency within the interval at which the information is to be monitored and the duration of the monitoring at each instance (e.g., for a twenty-four hour interval, a monitoring period of one minute at every ten minutes);

and other pertinent characteristics. The network visualization application begins extracting data from the network information files at the starting time and stops extracting data at the ending time. During each intermediate time interval, the visualization application compiles the information in the information file that meets the filtering criteria set forth by the system administrator, and stores the selected information for display at stated times or at the request of the administrator.

The visualization application displays a map of the network and dynamically overlays the map with graphical images that represent the selected information designated by the system administrator or other user. The information is presented in a dynamic, graphic (as opposed to numeric) manner that the user can quickly assimilate. For example, traffic between selected computers may be represented by lines whose width, color, density or other characteristic changes in accordance with the volume of traffic over time. By taking "snapshots" of this traffic at discrete intervals over a larger interval, one effectively forms "frames" that depict the traffic at various times and that, when played back one after the other in rapid succession, create a "movie clip" of the selected traffic flow parameters. This provides an environment in which the system administrator or other user can accurately and visually analyze the composition of network activity and thereby reduce human errors that occur during interpretation of static data tables that heretofore have been relied upon for presentation of network information.

## BRIEF DESCRIPTION OF THE DRAWINGS

The above and further advantages of the invention may be better understood by referring to the following description in conjunction with the accompanying drawings in which like reference numbers indicate identical or functionally similar elements:

Fig. 1 is a diagram of a network management system incorporating the invention;

Fig. 2 is a schematic diagram of the network reporting structure and how they interact with each other; and

Fig. 3 is an example of the steps performed by the network reporting structure in order to display the composition of network traffic to the user;

Figs. 4-A depicts a subset of Fig. 1 and a graphical image of the network activities between selected components on LAN 101 at time $_{t1}$;

Figs. 4-B depicts a subset of Fig. 1 and a graphical image of the network activities between selected components on LAN 101 at time $_{t2}$;

Figs. 4-C depicts a subset of Fig. 1 and a graphical image of the network activities between selected components on LAN 101 at time $_{t3}$; and

Figs. 4-D depicts a subset of Fig. 1 and a graphical image of the network activities between selected components on LAN 101 at time $_{t4}$.

## DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

Fig. 1 is a schematic diagram of a distributed network management system that is configured to share resources and data in accordance with the present invention. The illustrated system is a combination of four separate local area networks (LAN) 101-104 that are interconnected into a wide area network (WAN) 105 to form a single distributed network structure. Each LAN 101-104 may include servers and clients that are connected by physical media such as cables and network cards in order to share resources such as files or applications. A server may be a computer or process that provides shared network resources to network users, and a client may be a computer or process that accesses the shared network resources provided by the servers. Shared resources in a network may include printers and other peripherals, as well as software applications. The LANs 101-104 are interconnected to communicate with each other by routers 111-114. The routers exchange protocol-specific information between separate networks and determine the best path for sending data.

In order to effectively manage a distributed network system, the system administrator or other user must monitor network activity. Timely and accurate information about the states of each network component and the activities performed on each component is required for the system administrator to perform the necessary network manage-

ment functions. Therefore, the states of these network components are consistently monitored by a reporting structure which records the component's states and each network activity performed on those components.

The illustrative reporting structure 200 shown in Fig. 2 may reside in any location on the network. It includes a reporting application 202, three network information files 204-208 stored in one or more locations on the network, a network topology file, 209, and a visualization application 210 for extracting information from the network information files 204-208 and graphically displaying the information to the system administrator. The reporting application 202 constantly monitors the state of each network component and appends the results to the appropriate network information file 204-208. It also receives a record of each network activity and appends those to the information files 204-208. The records in the network information files 204-208 are time stamped to indicate when each record was generated. While the recording of network activity may be performed by a single reporting application 202, this task can also be performed without a reporting application. Each of the network components can append its state and activities directly to the appropriate network information files 204-208. The network files 204-208 are typically monitored and backed up by the system administrator and information in those files 204-208 may be deleted at the system administrator's discretion. The network topology file 209 records and stores the topology of the network at the times the network information files are generated.

In accordance with the present invention, after the network starts up, the user manually executes the visualization application 210 and uses the graphical user interface in the application to create filtering expressions for extracting the desired information from the network information files 204-208. The visualization application enables the user to obtain information about the overall network activities; to obtain information about activities between two or more network components; and to obtain information about each transaction performed on each network component. The user selects the appropriate filtering criteria from the graphical user interface associated with the visualization application 210. Based on the selected filtering criteria, the visualization application

210 selects the relevant data with the correct time stamp from the network information files 204-208, executes the filtering expression on selected data, calculates parameters that are associated with the selected data, and stores the calculated parameters in a local file 212. The topology of the network corresponding to this data is asssociated with it either directly in local file 212 or through links to the network topology file 209. Subsequently, when the user views the selected data through the visualization application 210, the visualization application 210 exhibits a map of the network and graphically displays the generated parameters through representational moving images that change with time to thereby represent changes in the underlying parameters as a function of time. Examples of representational moving images used by the visualization application 210 to display the generated parameters may include black and white or colored arrows, bar charts, graphs and other representational indicia whose length, width, density, color, or other visual or sensory characteristics vary in accordance with the desired parameters to be representationally displayed.

An example of a parameter of interest might be the number of log-in attempts made from a particular computer to others, or made to one or more computers in the network. These attempts may appropriately be represented by arrows directed from the computer of interest to the other computers in the network, or simply directed to the other computers, as the case may be. The arrows are shown in a dynamic fashion, e.g., as short directed segments traversing a portion of the screen during the display interval from or to one or more computers to indicate the "probing" nature of the log-in. The log in rate, i.e., the number of attempted log-ins during a given time interval, may be represented by the rate at which the arrow traverses the screen, or by the width or the arrow, or by the color, intensity or other changeable characteristic of the arrow or other representational element. The user may advantageously select the desired representational characteristics for the specified parameters, or they may be determined by default in the visualization application.

The visualization application 210 preferably maintains the selected files in the local files until the user decides to delete them. This enables the user to review the results from the reporting structure until the results are no longer needed.

Figs. 3 is an example illustrating the steps performed by the reporting structure 202 in order to generate a graphical display for the system operator. For example, if a "hacker", i.e., an unauthorized user, tries to obtain access to one or more computers on the network, the data in the reporting structure 200 accurately reports such information to the system operator in the following steps. In Step 310, the reporting application stores each log-in transaction performed by the hacker in the appropriate information files 204-208. Thus, for example, if the hacker uses the same user name with an excessive number of different passwords while trying to gain access to a single computer, the reporting structure will record each log-in transaction with each of the different passwords. As another example, if the hacker uses the same user name/password while trying to gain access to a number of different computers in the network, a record of each log-in transaction on each computer will be stored in the appropriate information files 204-208. During the network monitoring, the system operator or other user of the visualization application will be able to trace the changes in the destination computer by the hacker.

In Step 320, the user starts up the visualization application 210 and uses the graphical user interface in the visualization application to create filtering expressions for extracting the desired information from the network information files 204-208. The user selects the appropriate filtering criteria from the graphical user interface associated with the visualization application 210. In Step 330, the visualization application 210 selects the relevant data from the network information files 204-208; executes the filtering expression on selected data and stores the filtered data in a local file. In Step 340, the user restarts the visualization application 210 in order to monitor the network activities. In Step 350, the visualization application 210 displays a map of the network and overlays the map with a graphical display of dynamically changing images that represent the selected data over the selected time period.

Figs. 4-A to 4-D further illustrate how information is displayed to the system operator through the visualization application 210. Figs. 4-A to 4-D depict a subset of Fig. 1, each figure displaying LAN 101 and representational images of the network activities between selected components on LAN 101. According to the invention, the user may choose to view the activities on or between any network components. For instance, the user may choose to observe the network activities between components 402 and 408 passing through switch 410 Figs. 4-A to 4-D and thus portray network activities between components 402 and 408 for a selected period of time.

In particular, after selecting the appropriate information from the information files and generating the data corresponding with the selected information, the visualization application 210 displays a map of the network. In this case, the visualization application displays a subset of the network that depicts LAN 101. The visualization application 210 then dynamically overlays the map with graphical images that symbolize the generated data. In Figs. 4-A to 4-D, double sided arrows are used as the graphical images. At time $t_1$, the visualization application 210 displays medium width, double sided arrows between components 402 to 408, as shown in Fig. 4-A. This portrays a moderate amount network traffic between these network components during the time subinterval corresponding to $t_1$. At time $t_2$, Fig. 4-B, the arrows between components 402 and 408 have a smaller width to graphically illustrate less network traffic. At time $t_3$, Fig. 4-C, the arrows between these components are considerably thicker and graphically denote more network traffic than at times $t_1$ and $t_2$; finally, at time $t_{4, Fig}$. 4-D, the arrows between computers 402 and 408 are again narrower, thus depicting a moderate amount of network activities between components 402 and 408. Figs. 4-A to 4-D therefore give the user a visual, dynamic display of the network activities that is instantly assimilable and that does not require the user to analyze massive amounts of data in static tables.

The foregoing description has been directed to specific embodiments of this invention. It will be apparent, however, that other variations and modifications may be made to the described embodiments, with the attainment of some or all of their advan-

tages. Therefore, it is the object of the appended claims to cover all such variations and modifications as come within the true spirit and scope of the invention.

What is claimed is: